404 – Steganography – Level 4

Team Information	
Team Name:	Barely Legal
Results Email:	[redacted]
Examination Time Frame:	to 10/31/08

Instructions

Description: Examiners must develop and document a methodology used to extract and decrypt the data hidden with Steganos in each of the bitmap files in the **404_Steganography_Level4_Challenge2008** folder into English language documents.

For each file name provide the hidden data or password and a detailed explanation of your process (software or technique) used to examine and determine your results.

Report with the filename, the exact detailed explanation of your process (software or technique) used to examine and detect the information, and then to successfully extract the information.

Total Weighted Points: 80 Total Points available per entry – Total 400 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

Internal Reviewer Use Only

Reviewer:		Points Awarded:	
Date:		Review Period:	to
Completed:	☐ Yes ☐ No ☐ Partial		

REPORT OF EXAMINATION

404 – Steganography Level 4

All images were identified as files that may contain steganography embedded using the Least Significant Bit technique

Signature for GhostHost v1.0 found in file "File2.bmp"

Additional analysis with the "LSB Enhancement" process of Stegalyzer was performed, but unable to find embedded data in any of the host files.

METHODOLOGY / NOTES FORM

404 – Steganography Level 4

Date / Time	Notes
31-Oct-08 6:30 pm	Tool(s) Used: StegSpy by spyHunter (www.spy-hunter.com) Stegalyzer SS (30-day trial) by Backbone Security (www.sarc-wv.com) All images were identified as files that may contain steganography embedded using the Least Significant Bit technique Signature for GhostHost v1.0 found in file "File2.bmp" Additional analysis with the "LSB Enhancement" process of Stegalyzer was performed, but unable to find embedded data in any of the host files .